



# INTERNET, INTRANET, AND E-MAIL OPERATIONS

**FC No.: 1401**

**Date: 08/15/08**

If a provision of a regulation, departmental directive, rule, or procedure conflicts with a provision of the contract, the contract prevails except where the contract provision conflicts with State law or the Police Collective Bargaining Law. (FOP Contract, Article 61)

## Contents:

- I. Purpose
- II. Applicability
- III. Policy
- IV. CALEA
- V. Proponent Unit

### **I. Purpose**

This is Montgomery County's policy (hereafter referred to as the "Policy") regarding proper use of Internet/intranet access and electronic mail (e-mail) systems provided by the county for the use of all department employees (hereafter referred to "employees"). "Employer" means the County Executive and designees.

Nothing in this policy is intended to imply or constitute a waiver of an employee's constitutional, contract, or statutory rights.

Internet/intranet access and e-mail systems are provided for employees and persons legitimately affiliated with the business of the county government for the efficient exchange of information and the completion of assigned responsibilities.

### **II. Applicability**

The provisions of this policy apply to all department employees.

### **III. Policy**

Internet/intranet access and e-mail systems are provided to employees for use in conducting the county's official business. Unless an exception is specifically approved by the employer, employees are expected to use these resources responsibly and professionally, and must not use Internet/intranet access or e-mail systems in a manner that violates any federal, state, or county law, county regulation, or departmental directive. Although the use of county provided Internet/intranet access or e-mail systems for personal use is discouraged, it is recognized that circumstances sometimes arise that necessitate personal use of these systems. Such use is to be kept to a minimum and should not disrupt the conduct of service or performance of official duties. Employees are to devote their entire working time to the performance of their duties. Employees may make reasonable and limited personal use of county-provided Internet/intranet access or e-mail systems in accordance with this policy. Employees who violate this policy may be subject to disciplinary and other actions under section III.D of this policy.

#### **A. Internet, Intranet, and E-Mail Connections**

Connections to county-provided Internet/ intranet access or e-mail systems must be made only in the following manner:

1. PC's (desktops and laptops) connected to the county's computer network ("network") may connect to the Internet only via the county's secure central Internet service connection.
2. Stand-alone (non-network-connected) PC's do not have access to the county's secure central Internet service connection; therefore, stand-alone PC's may connect to the Internet through a private Internet Service Provider (ISP), such as America On-Line (AOL). Stand-alone PC's connecting to the Internet must have active, up-to-date, anti-virus software. If a stand-alone PC has been connected to an Internet service, and is now being added to the county network, the using department must check the entire data contents of the PC for viruses before connecting it to the network.
3. Costs incurred by the county for ISP connections to stand-alone PCs are the responsibility of the using department and must be in accordance with that department's policy. Employees must obtain department approval prior to obtaining a county provided ISP connection.

**B. Inappropriate Use**

The following conduct is prohibited by this directive:

1. Sending, forwarding, storing, or saving on any county PC or server any material:
  - a. The possession of which is illegal, or that advocates illegal conduct.
  - b. That is obscene or pornographic as defined by law.
  - c. That is untruthful, non-job related, and defamatory.
  - d. That knowingly advocates that an employee disobey a lawful direct order from a supervisor.
  - e. That knowingly advocates the violation of county laws, or department regulations, procedures, or policies.
  - f. That when viewed or heard by other employees, causes actual or significant disruption to the efficiency of a work unit.
  - g. That threatens or advocates physical harm to an individual or threatens the safety of the public.
  - h. That threatens or advocates physical damage to personal or real property.
  - i. That advocates unlawful discrimination against an individual on the basis of race, color, creed, sex, marital status, religion, country of origin, age, sexual orientation, or disability.
  - j. That expresses clearly racist or discriminatory sentiments regarding race, color, creed, sex, religion, country of origin, age, sexual orientation, or disability.
  - k. That is reasonably perceived as constituting unlawful harassment.
  - l. That threatens or advocates the violent overthrow of the government.
2. Using the county's Internet/intranet access or e-mail systems in connection with secondary employment or for personal financial or commercial gain.
3. Using the county's Internet/intranet access or e-mail systems to gain unauthorized access to resources via the Internet or intranet.
4. Using the county's Internet/intranet access or e-mail systems for gambling or any illegal activities.
5. Infringing upon computer software and data protected by copyright and license laws.
6. Sending broadcast messages to all county e-mail users without obtaining prior approval from the CAO's designee who administers the county's e-mail system for broadcast messages.
7. Connecting a PC to the county's computer network in a manner that is not authorized by section III.

The prohibitions stated above do not apply to an employee's use of the county-provided Internet/intranet access and e-mail systems for purposes of the conduct of official business, including police investigations.

**C. Ownership, Privacy, and Monitoring**

All county-provided electronic systems, hardware, software, temporary or permanent files, and any related systems or devices used in the transmission, receipt, or storage of Internet, intranet, or e-mail communications are the property of, or are licensed to, the county. All electronic communications generated by employees using the county's Internet/intranet access and e-mail systems, or downloaded and stored on the county's computer resources, are the property of the county and, therefore, are not considered

private. This includes e-mail from an employee's personal account, such as Hotmail or AOL, if that e-mail is accessed and stored on the county's computer resources. E-mail messages and electronic files may be retrieved from storage by the county and its agents without prior notice, even if messages and files have been deleted by the sender and receiver. These messages and files may be used in disciplinary or other proceedings. Furthermore, appropriate measures must be taken by employees to prevent unauthorized access to confidential information when using the county's Internet/intranet access and e-mail systems.

To the extent not prohibited by law, the county may monitor employees' use of county provided Internet/intranet access and e-mail systems and access employees' e-mail messages and computer files at its sole discretion. This includes e-mail messages from an employee's personal e-mail account, such as Hotmail or AOL, if the personal e-mail uses the county's computer resources. The department may monitor and access employees' use of county-provided Internet/intranet access and e-mail systems in connection with the conduct of a criminal investigation of the employee's activities.

To the extent not prohibited by law, and only after an Internal Affairs Division (IAD) case is opened and a case number assigned, IAD may monitor and access employees' use of county-provided Internet/intranet access and e-mail systems when the Director, Internal Affairs Division, reasonably suspects that an employee's e-mail messages and computer files contain evidence that the employee has committed a crime, or that the employee has committed an act that subjects the employee to disciplinary action under applicable laws, applicable regulations, applicable departmental directives, or the provisions of this policy.

In certain situations, the county may be compelled to access and disclose to third parties messages sent over its Internet, intranet, or e-mail systems. The Maryland Public Information Act (MPIA), Maryland Code Ann., State Gov't Art. §§ 10-6111 to 10-628 (1998 Repl. Vol.) applies to an electronically stored e-mail message or a hard copy of the message in the custody and control of a public officer or employee, if the message is related to the conduct of public business. 81 Op. Att'y Gen., Op No. 96-016, 1996 WL 305985 (1996).

System administrators in DTS or other county departments may access an employee's e-mail messages and computer files related to an employee's use of the county's Internet/intranet access and county e-mail systems, even though the employee uses a privately held password to access the employee's county-owned computer and e-mail. The existence of passwords and "message delete" functions do not restrict or eliminate the county's ability or right to access electronic communications.

To the extent permitted by law, the county may monitor and control the flow of Internet/intranet and e-mail traffic over the county's network for security and/or network management reasons or other business purposes.

The employee's use of the Internet, intranet and e-mail systems indicates consent to this policy, and to the county's review of the employee's electronically stored e-mail messages and computer files related to the employee's use of the county's Internet/intranet access and e-mail systems.

D. Enforcement of Policy

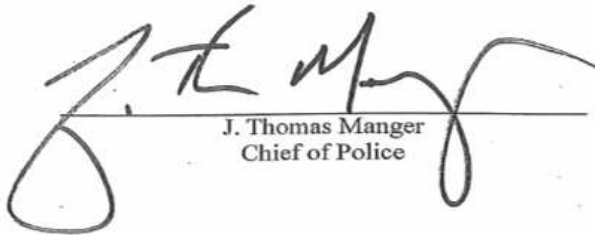
1. Employees are responsible for ensuring that their use of county-provided Internet/ intranet access and e-mail is in accordance with this Policy.
2. The Police Department is responsible for enforcing employees' compliance with the provisions of this policy, and for investigating non-compliance.
3. Employees who violate this policy may be subject to disciplinary action, up to and including dismissal, in accordance with Montgomery County laws and applicable regulations, including applicable Personnel laws, Ethics Laws, and Ethics Regulations, and the FOP collective bargaining agreement. If a violation of this policy constitutes a crime, the violator may be subject to prosecution. The county also reserves its right to pursue other legal remedies to obtain reimbursement from employees if a

violation of this policy results in a financial loss to the county, or results in a financial obligation owed by the county.

4. Employees must not access another user's e-mail account without authorization from the employer or the employee to whom the e-mail account is assigned.
5. Employees must obtain department approval prior to acquiring a county-provided ISP connection for a stand-alone PC.
6. Prior to sending a broadcast message to all county e-mail users, employees must obtain approval in accordance with the Electronic Broadcast Policy and Procedures (available through DTS).
7. This policy shall be administered fairly, equitably, and consistently both within the unit and with the county's general policy to the extent that policy is not inconsistent with this one.

**IV. CALEA:** None

**V. Proponent Unit:** Technology Division



J. Thomas Manger  
Chief of Police